AfricaCERT 15: The Road to Maturity Report

Presented by AfricaCERT.

AfricaCERT - 2019

Executive Summary.

AfricaCERT organized five days of capacity building focused on creation and maturity of Computer Security Incident Response teams (CSIRTS). AfricaCERT also helped organize the Internet Infrastructure Day in partnership with the Global Forum of Cyber Expertise, the West and Central African Research and Education Network, the African Network Operator Group, the Internet Society and other African Organisations for Internet Governance. The AfricaCERT 15 workshop was held from 09 to 16 June 2019 in Sheraton Hotel, Kampala in Uganda during the Internet Africa Summit https://www.internetsummit.africa/en/. The AfricaCERT workshop attracted 46 participants from 16 African countries. Seven participants attended closed online streaming sessions that were labelled traffic light protocol white.

Why CSIRT Maturity?

African governments are involved in the creation and management of governmental and national CSIRTs as information sharing platforms and coordination bodies within their countries. Major initiatives are also supported at the regional level by Regional Economic commissions and the African Union. In addition, African organisations are creating Computer Security Incident Response Teams for coordinating the response to their organization's computer security incidents.

With a growing number of initiatives to establish Computer Security Incident Response Teams within Africa are also many false starts. It became necessary to provide tools and frameworks to help teams assess how well they govern, document, perform, and measure, their CSIRT services and return value to their stakeholders.

AfricaCERT 15 was tasked to respond to the challenges faced by many starting teams and teams in operation with the goal to tackle challenges and discuss opportunities. International experts from Estonia, France, Japan and the Netherland were invited to share their experience and lessons learned with their colleagues from Africa. Teams also discussed and approved the new AfricaCERT Framework. AfricaCERT welcomed a new operational member: the CSIRT Team of Ghana National Communications Authority (NCA CERT).

Survey results and the lessons learned that were discussed outlined few areas of improvement for future AfricaCERT meetings. Providing opportunities for remote participation for attendees and speakers was greatly appreciated, AfricaCERT was asked to make it possible for future events. Funding for travel and event organization was a major issue that the Secretariat has been instructed to tackle.

Jean-Robert Hountomey.
Executive Director
Global Coordination

AfricaCERT organized five days of capacity building focused on creation and maturity of Computer Security Incident Response teams (CSIRTS). The meeting was organized in two tracks: Technical track and Management track.

Schedule

The event was organized around key topics to meet the existing needs of teams:

CSIRT Bootcamp.

- CSIRT fundamentals (AfricaCERT)

Management and Technical Tracks.

- Securing Webserver (Team Cymru)
- Opensource Intelligence (JPCERT)
- Opensource tooling for the CSIRT (TunCERT and AfricaCERT)
- CSIRT Maturity workshop: Stimulating the development and maturity enhancement of African CSIRTS (Opencsirt foundation, Don Stikvoort, AfricaCERT)
- Practical CSIRT Study (TunCERT, AfricaCERT)
- Incident response workshop (RIA, ANSSI France, CERT.EE, Cyber4DEV)

CSIRT Day (Hosted by African CSIRTs and AfricaCERT Members)

Side Meetings

Also, AfricaCERT partnered with other African Institutions to host the Global Forum of Cyber Expertise Internet Infrastructure Day.

CSIRT fundamentals

The course is based on FIRST CSIRT Basic course and aimed to define incident management and establish the need for a Computer Security Incident Response Team. The course also discusses the purpose and structure of CSIRTs and a high-level overview of the key issues and decisions that must be addressed in establishing and maintaining a CSIRT.

Securing Webserver

AfricaCERT stats on incident in Africa still show an increasing number of incidents related to website intrusion and malware propagation. In addition, a relatively large number of African websites don't use encryption. The workshop was organized to teach stakeholders strategies to identify vulnerabilities in their websites and to secure the webserver. The workshop was based on the manipulation and configuration of open source software and structured around tools, including: removing unnecessary services, enabling automatic security updates, blocking clients that fail to authenticate correctly with your services repeatedly, hardening webservers, web application firewall, mod_evasive, chrooting, generating, config and testing ssl certificate including using certificates from Let's Encrypt, a free, automated, and open certificate authority (CA).

Opensource Intelligence

The session on Open Source Intelligence (OSINT) Techniques focused on providing information and resources to conduct open source internet research for an Investigator, Analyst, Researcher.

Opensource tooling

AfricaCERT's approach for CSIRT operation also includes a close look at the processes and the technology including tooling. AfricaCERT focuses on opensource tools to educational, funding and resource constrained challenges. The session drove from the experience of the successful operation of a mature African team using only opensource tools for all services and the lessons learned from their experience.

CSIRT Maturity workshop: Stimulating the development and maturity enhancement of African CSIRTS.

The CSIRT Maturity Workshop aimed to help organisations to evaluate and improve the maturity of their computer emergency response team (CSIRT). Activities conducted were:

- sharing evaluation instruments to identify the strengths and weaknesses of teams;
- performing individual and group exercises focused on behavior in CSIRT teams;
- exchanging experiences with other participants.

Incident response workshop

The workshop focused on the operational, tactical, procedural, legal and communication aspects of incident response. The whole incident response lifecycle was covered from incident detection through various escalation levels until the implementation of mitigation measures and post-incident activities. This includes incident response best practices, workflow, classification, SLAs and team composition/roles along with business impact. Internal and external incident communication was also covered including compliance and supervision, as well as risk management and their role in incident handling.

CSIRT Day.

The CSIRT Day provides the opportunity for CSIRT Teams to give update on their operations, discuss challenges and opportunities and sets the discussion topics for future meeting. It is also the opportunity for teams to exchange further, lesson learned.
To fulfill a previous request from African CSIRT teams, AfricaCERT organized a workshop with AfriNIC on AfriNIC Whois database for Incident Responders. The purpose of the workshop was to make CSIRT teams more familiar with AfriNIC whois and the queries to extract relevant information. AfricaCERT also organized a workshop with CyberGreen as continued discussion from previous session on how to motivate decision makers to adapt right actions and policies on a country's Cyber Ecosystem healthiness. It also provides recommendations on ways to improve cyber health by informing CSIRTs and policy makers on the most significant systemic risks and reflect on how to adapt security measures and policies. CyberGreen also started national level ecosystem health-check analysis with its technical partners - analyzing not only the level of

DDoS infrastructure, but email infrastructure and internet routing infrastructure. Comments and suggestions from the audience outlined how the platform could be used by National CSIRT to drive Cyber Ecosystem healthiness.
Membership drive.
During the CSIRT Day, AfricaCERT welcomed the CSIRT Team of Ghana National Communications Authority (NCA CERT) as new operational member. The membership of NCA CERT was supported by bjCSIRT, National CSIRT of Benin Republic and TunCERT, Tunisian Computer Emergency Response Team.

Team of Instructors are/from:
AfricaCERT
CERT Estonia
French Cybersecurity Agency (ANSSI France)
JPCERT/CC – Japan Computer Emergency Response Team Coordination Centre
OpenCSIRT foundation
Team Cymru
TunCERT – Tunisian Computer Emergency Response Team
Clarified Security (Estonia)

Participants
The AfricaCERT workshop attracted 46 participants from 16 African countries. Seven participants attended closed streamed sessions.

GFCE Triple I Capacity Building Day | The Internet Infrastructure Security Day

The workshop was focused on Open Internet Standards adoption and how to develop and commit to specific actions that will help improve the African Region Internet Economy. More information in the GFCE website.
https://www.thegfce.com/initiatives/i/internet-infrastructure-initiative/documents/reports/2019/06/16/gfce-triple-i-kampala-report

Side Meetings

ICANN Day.
The Africa Internet Summit (AIS) is an annual, regional, multi-stakeholder ICT conference. It is the pinnacle educational and business ICT event in Africa where key players in the Internet industry can interact with the global Internet community. AfricaCERT was invited to make a presentation on June 16, 2019 during the ICANN Day https://features.icann.org/event/icann-speaking-events/icann-day-ais-2019.

AfGWG.
The AFRINIC Government Working Group (AfGWG) was set up at the initiative of AFRINIC to work with African governments and regulators to address general internet governance challenges in Africa. AfricaCERT made a presentation on CSIRT for Policy Makers June 17, 2019. Content of the AfricaCERT presentation was taken from policy perspectives in African economies but also from the course Incident Handling for Policy makers released by the Forum of Incident Response and Security Teams (FIRST). https://www.first.org/education/trainings

AfREN Forum.

AfricaCERT was invited at the Africa Research and Education Networking (AfREN) held its annual forum on June 17th, 2019. AfREN is the annual forum on African research and education networking. As one of the Af* organizations, the AfREN forum is part of the annual Africa Internet Summit (AIS) and was convened since 2007 by the Research and Education Networking Unit (RENU) of the Association of African Universities in collaboration with AfNOG & AFRINIC.

Acknowledgement

AfricaCERT expresses its gratitude to the presenters, the participants and the organisations that made AfricaCERT 15 possible. We would like to thank AfNOG, AfriNIC, ISOC, ICANN, AIS, TunCERT, JPCERT/CC, French national cybersecurity agency – (ANSSI), Estonian Information System Authority, CERT Estonia, Clarified Security, OpenCSIRT foundation, Team Cymru, Cyber4Dev, CERT.UG, UGCERT and all the CSIRT Teams.
AfricaCERT 15 would not have been possible without the help of the AfricaCERT Elders: NII Quaynor, Alain Aina, Emmanuel Adjovi. We also thank Marcus Adomey, Nancy Dotse and her Team, Badru Ntege, Don Stikvoort, Martin Karungi, Ronald Bakakimpa, Koichiro Komiyama, Liina Areng, Martin Indrek Miller, Anthony Munos, Pierre Giordanengo, Sherif Hashem, Naoufel Frikha, Nabil Sahli, Emmanuel Thekiso, Moctar Yedali and Auguste Yanke. AfricaCERT also thanks ISOC Africa Team (Dawit Bekele, Michuki Mwangi, Kevin Chege) for their support and help with remote participation.